09-17-04 IFW

Express Mailing Label No. EV 380179533 US

Docket No. 971-28-001 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: O. ATSUMI et al.

Serial No. 10/692,483 Art Unit: 2131

Filing Date: October 23, 2003

For: RANDOM NUMBER GENERATION APPARATUS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

Sir:

Transmitted herewith is a certified copy of the priority document in accordance with 35 USC 365(c).

If any additional fee is required, charge Deposit Account No. 11-1580. A duplicate of this transmittal is attached.

Respectfully submitted,

September 15, 2004

Steven C. Patrick
Registration No.40,341
Attorney for Applicant

KOPPEL, JACOBS, PATRICK & HEYBL
555 St. Charles Drive, Suite 107
Thousand Oaks, California, 91360
Telephone: (805) 373-0060

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service via Express mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

9/15/04 Marianne Middleton

Date Marianne Middleton

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/692,483
Applicants : O. Atsumi et al.
Filed : October 23, 2003
TC/A.U. : 2131
Docket No. : 971-28-001
Title: RANDOM NUMBER GENERATION APPARATUS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT IN ACCORDANCE WITH 35 USC 365(c)

Sir:

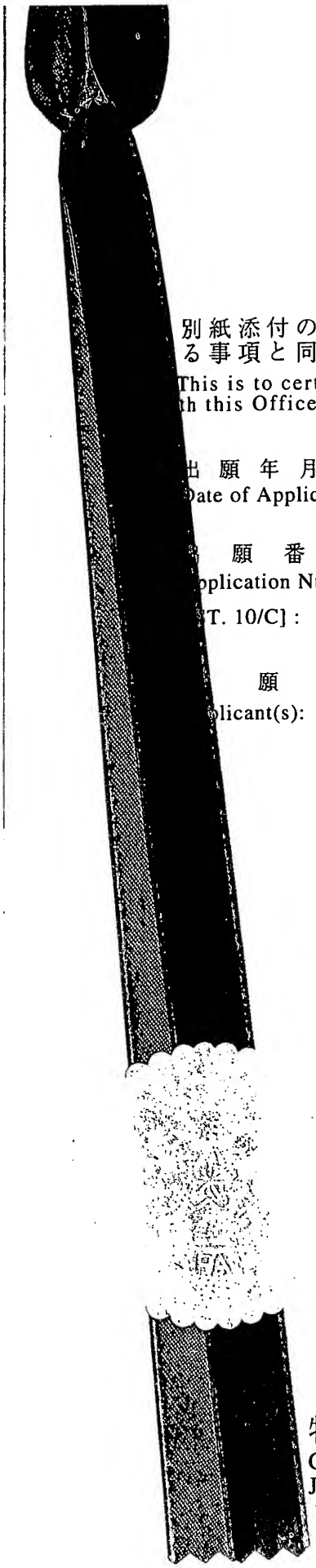
Please find enclosed a certified copy of the priority document - Japanese patent application no. 163428/2001, filed in Japan on April 24, 2001 - cited for the patent application identified above.

Respectfully submitted,

September 15, 2004

Steven C. Patrick
Registration No. 40,341
Attorney for Applicant

KOPPEL, JACOBS, PATRICK & HEYBL
555 St. Charles Drive, Suite 107
Thousand Oaks, California 91360
(805)373-0060



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００１年　４月２４日

出願番号
Application Number: 特願２００１－１６３４２８

[ST. 10/C]: [ＪＰ２００１－１６３４２８]

出願人
Applicant(s): 株式会社三技協
株式会社サンテクト

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年　８月　９日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

BEST AVAILABLE COPY

出証番号　出証特２００４－３０７０９４７

【書類名】　特許願
【整理番号】　SA01-02
【あて先】　特許庁長官殿
【提出日】　平成13年 4月24日
【国際特許分類】　H04I 19/28
【発明者】
　【住所又は居所】　神奈川県相模原市北里２－１７－２７
　【氏名】　三田　二三夫
【発明者】
　【住所又は居所】　神奈川県相模原市上鶴間２－８－３８
　【氏名】　渥美　治
【特許出願人】
　【識別番号】　595095353
　【氏名又は名称】　株式会社三技協
【特許出願人】
　【識別番号】　500459292
　【氏名又は名称】　株式会社サンテクト
【代理人】
　【識別番号】　100071098
　【弁理士】
　【氏名又は名称】　松田　省躬
【手数料の表示】
　【予納台帳番号】　039240
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】　明細書

【発明の名称】　乱数発生装置

【特許請求の範囲】

【請求項１】　物理的な雑音を測定してランダム雑音を発生するランダム雑音発生手段と、

このランダム雑音を波形整形してランダムパルス波を生成するランダムパルス波生成手段と、

このランダムパルス波を一定周期のクロックでサンプリングしてサンプル値のオン・オフをパルス符号とする一定周期の２値パルス列に変換する２値パルス列変換手段と、

この２値パルス列の極性を一定周期おきに反転させて所定の単位符号長における１／０符号の出現バランスを平滑化する２値パルス列符号平滑化手段と、

を備え、

前記２値パルス列符号の乱数列を発生してなる乱数発生装置。

【請求項２】　前記ランダム雑音の発生間隔をパルスのオン・オフ時間として前記ランダムパルス波を生成してなる請求項１記載の乱数発生装置。

【請求項３】　前記ランダム雑音発生手段を複数用いて合成したランダム雑音を前記ランダムパルス波生成手段に入力して前記ランダムパルス波のオン・オフの発生頻度を増大させてなる請求項１記載の乱数発生装置。

【請求項４】　前記ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成してなる請求項１記載の乱数発生装置。

【請求項５】　前記２値パルス列符号平滑化手段を前記クロックの周波数を１／２に分周する１／２分周器とマルチプレクサまたはＸＯＲゲートで構成してなる請求項１記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ用のＩＤパスワードや各種暗号鍵などに使用する

ための乱数を発生する乱数発生装置に関する。

【０００２】

【発明が解決しようとする課題】

ＩＤパスワードや各種暗号鍵などの安全性を高めるには、１／０の出現確率が各々１／２の等確率で、各ビットが他と独立してビット間に相関のない真正乱数を使用する必要がある。

真正乱数は、実際にサイコロやコインを振るわけにもいかないので、電気的な雑音の電圧変化を測定するなどの物理乱数を用いて生成することが多いが、物理乱数をそのまま用いても真正乱数とはならない。

【０００３】

物理乱数のビット列は、１／０が無規則に出現するが、１／０の出現バランスは不確定さを持つためインバランスとなる。

そのため、物理乱数のインバランスを解消する方法として、出力パルス列の積分値を乱数生成側にフィードバックして雑音レベルを制御したり、出力パルス列をシフトレジスタに入力してパラレル変換したパルス列の論理和を求めて乱数を生成するなどの方法が提案されている。

ところが、いずれの方法も偶然性に支配される要素が多いため、確実に１／０の出現バランスを等確率にすることは困難であった。

【０００４】

そこで本発明は、偶然性に支配されることなく物理乱数のインバランスを解消して確実に１／０の出現バランスを等確率にできる乱数発生装置を提供することを目的になされたものである。

【０００５】

【課題を解決するための手段】

かかる目的を達成するために、本発明は以下のように構成した。

すなわち、請求項１の発明は、物理的な雑音を測定してランダム雑音を発生するランダム雑音発生手段と、

このランダム雑音を波形整形してランダムパルス波を生成するランダムパルス波生成手段と、

このランダムパルス波を一定周期のクロックでサンプリングしてサンプル値のオン・オフをパルス符号とする一定周期の２値パルス列に変換する２値パルス列変換手段と、

この２値パルス列の極性を一定周期おきに反転させて所定の単位符号長における１／０符号の出現バランスを平滑化する２値パルス列符号平滑化手段と、

を備え、

前記２値パルス列符号の乱数列を発生してなる乱数発生装置である。

【０００６】

請求項２の発明は、前記ランダム雑音の発生間隔をパルスのオン・オフ時間として前記ランダムパルス波を生成してなる請求項１記載の乱数発生装置である。

請求項３の発明は、前記ランダム雑音発生手段を複数用いて合成したランダム雑音を前記ランダムパルス波生成手段に入力して前記ランダムパルス波のオン・オフの発生頻度を増大させてなる請求項１記載の乱数発生装置である。

請求項４の発明は、前記ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成してなる請求項１記載の乱数発生装置である。

請求項５の発明は、前記２値パルス列符号平滑化手段を前記クロックの周波数を１／２に分周する１／２分周器とマルチプレクサまたはＸＯＲゲートで構成してなる請求項１記載の乱数発生装置である。

【０００７】

【発明の実施の形態】

以下に図面を参照して本発明の実施の形態について説明する。

図１に、本発明を実施した乱数発生装置のブロック図を示す。

また、各ブロックの信号波形とそのタイミングチャートを図２に示す。

乱数発生装置は、雑音源１が発生する周期性のないランダム雑音ｎを波形整形回路２に入力してランダムパルス波ｐ１を生成する。

【０００８】

次に、ランダムパルス波ｐ１と発振器３のクロックｃ１をサンプル＆ホールド回路４に入力して一定周期の２値パルス列ｐ２を生成する。

そして、２値パルス列ｐ２とクロックｃ１を分周器５で１／２に分周した１／２分周クロックｃ２をスイッチング回路６に入力して２値パルス列ｐ２の極性を１周期おきに反転させ、１／０符号の出現バランスを平滑化した平滑２値パルス列ｐ３を出力する。

【０００９】

雑音源１は、熱雑音、ショット雑音、電子なだれなどによる白色雑音を物理的な雑音の発生源とする。

【００１０】

波形整形回路２は、ランダム雑音ｎを対数増幅回路で所定の電圧レベルに増幅し、これをコンパレータに入力してトリガレベル以上の雑音波形をトリガパルスとして取り出す。

そして、これを単安定マルチバイブレータに入力して外付けのＣＲによって決まる所定のパルス幅を有するランダムパルス波ｐ１を生成する。

このときのパルス幅は、サンプリング定理によりクロックｃ１のパルス幅の２倍以上に設定する。

また、このときのトリガパルスはランダムパルス波ｐ１の立ち上がり、もしくは立ち下がりのエッジ部分となり、トリガパルスの幅が長くなったり短くなったりしても一定のパルス幅を得ることができる。

【００１１】

ランダム雑音ｎの発生間隔にばらつきがある場合は、トリガパルスをＴ入力のたびにＱ出力が反転するＴ－ＦＦ２進カウンタに入力してトリガパルスの発生間隔をパルスのオン・オフ時間とするランダムパルス波ｐ１を生成してもよい。

これにより、ランダムパルス波ｐ１のオン・オフ時間の割合を均等にすることができる。

【００１２】

乱数の発生を高速化する場合は、複数の同一あるいは多種類の雑音源１の出力を合成し、波形整形回路２を介してサンプル＆ホールド回路４に入力する。

これにより、ランダム雑音ｎの発生頻度を増大させてランダムパルス波ｐ１のオン・オフの切換えを頻繁にする。

この場合、ランダム雑音ｎの発生頻度に応じてクロックｃ１の周期を短くし、クロックｃ１の周期に応じてランダムパルス波ｐ１のパルス幅を適正な長さに調節する必要がある。

【００１３】

サンプル＆ホールド回路４は、図３に示すように、ＦＦを２個使用してＣ入力は入力側のＦＦに直接、出力側のＦＦにはインバータを介して反転したクロックｃ１を供給する。

これにより、Ｃ入力のアップエッジで入力側のＦＦに記憶されたＤ入力のランダムパルス波ｐ１のオン・オフは、出力側のＦＦのＣ入力が“０”なのでそのまま出力側のＦＦのＱ出力に転送され、Ｃ入力のダウンエッジでは出力側のＦＦのＣ入力がアップエッジになるのでＱ出力を保持し、次のＣ入力のアップエッジまでその状態を変えずにいる。

このため、Ｃ入力のアップエッジでランダムパルス波ｐ１のオン・オフ状態を記憶した２値パルス列ｐ２がクロックｃ１の１／２の周期でクロックｃ１に同期して出力される。

【００１４】

分周器５は、Ｔ－ＦＦのＴ入力にクロックｃ１を２発入力するたびにＱ出力を元の状態に戻してクロックｃ１を１／２に分周する。

あるいは、図４に示すように、Ｄ－ＦＦの反転Ｑ出力をＤ入力に接続してＤ－ＦＦをＴ－ＦＦとして動作させてもよい。

このとき、反転Ｑ出力が次のＤ入力となるので、Ｃ入力のあるたびにＱ出力が反転する。

【００１５】

スイッチング回路６は、図５に示すように、２個のＡＮＤゲートとＯＲゲートおよびインバータを組み合わせたマルチプレクサで構成し、１／２分周クロックｃ２を制御入力として制御入力の“１”または“０”により２値パルス列ｐ２の正相出力と逆相出力のいずれか一方を選択して平滑２値パルス列ｐ３を出力する。

あるいは、図６に示すように、２値パルス列ｐ２と１／２分周クロックｃ２を

ＸＯＲゲートに入力して両者を排他的論理和で加算し、１／２分周クロックｃ２の１／０に同期して２値パルス列ｐ２の符号を１周期毎に正逆転させて平滑２値パルス列ｐ３を出力してもよい。

なお、実施例では１／２分周により正相出力と逆相出力を切換える方法をとっているが、分周度合いを高めて所定の単位符号長における１／０符号の出現バランスを平滑化する方法も実施可能である。

【００１６】

【発明の効果】

以上説明したように、本発明の乱数発生装置は、ランダム雑音を波形整形してランダムパルス波を生成し、これをクロックでサンプリングして一定周期の２値パルス列に変換し、その極性を一定周期おきに反転させて２値パルス列符号の乱数列を発生する。

従って、本発明によれば、通常、２値パルス列の１／０の出現バランスは、雑音の発生頻度に左右されるのでインバランスとなるが、このように２値パルス列の極性を一定周期おきに反転させると、符号配列のインバランス性が平滑化されて確実に１／０の出現確率がおのおの１／２に近い２値パルス列が得られる。

【００１７】

例えば、２値パルス列を“０１１０００１１００１１１００００１００”とすると、１／０の出現確率はおのおの８／２０と１２／２０となり“０”に偏っているが、その極性を１周期おきに反転させると“００１１０１１００１１０１１０１０００１”となり、１／０の出現確率はおのおの１０／２０と１０／２０で、１／２あるいはそれに近い値となる。

【００１８】

また、本発明の乱数発生装置は、ランダム雑音の発生間隔をパルスのオン・オフ時間としてランダムパルス波を生成する。

従って、本発明によれば、通常、ランダムパルス波のオン・オフ時間の割合は、雑音の発生頻度に左右されるのでいずれか一方に偏るが、このようにランダム雑音の発生間隔をパルスのオン・オフ時間とすると、その割合を均等にすることができる。

【００１９】

また、本発明の乱数発生装置は、ランダム雑音発生手段を複数用いて合成したランダム雑音をランダムパルス波生成手段に入力してランダムパルス波のオン・オフの発生頻度を増大させる。

従って、本発明によれば、ランダムパルス波をサンプリングして生成する２値パルス列の周波数をランダムパルス波のオン・オフの発生頻度に応じて高くできるので、乱数の発生をより高速化できる。

【００２０】

また、本発明の乱数発生装置は、ランダムパルス波生成手段を対数増幅器とコンパレータおよび単安定マルチバイブレータまたはトグルフリップフロップで構成する。

また、２値パルス列符号平滑化手段をクロックの周波数を１／２に分周する１／２分周器とマルチプレクサまたはＸＯＲゲートで構成する。

【００２１】

従って、本発明によれば、デジタル回路を主体に装置を構成できるので、微弱信号を扱うアナログ回路の部分が少なくなり、外乱などの影響を受け難くなって装置の信頼性が向上する。

また、回路が簡素化され、アナログ的な調整もほとんど不要になるので、製造コストを低減すると共に、量産化も容易になる。

【図面の簡単な説明】

【図１】

本発明を実施した乱数発生装置のブロック図である。

【図２】

図１の各ブロックの信号波形とそのタイミングチャートである。

【図３】

本発明を実施したサンプル＆ホールド回路の論理図である。

【図４】

本発明を実施した分周器の論理図の変形例である。

【図５】

本発明を実施したスイッチング回路の論理図である。

【図６】

本発明を実施したスイッチング回路の論理図の変形例である。

【符号の説明】

1　雑音源

2　波形整形回路

3　発振器

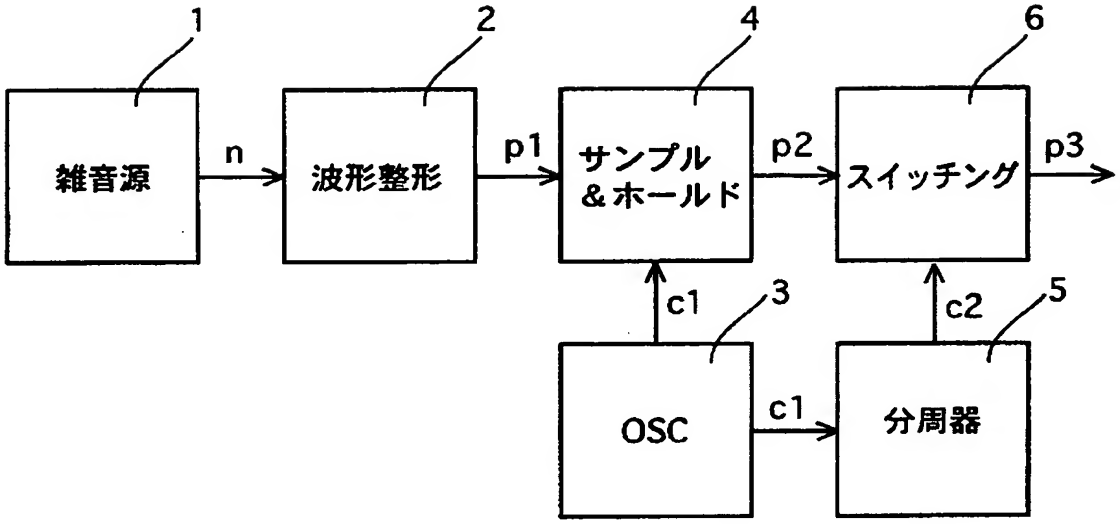
4　サンプル＆ホールド回路

5　分周器

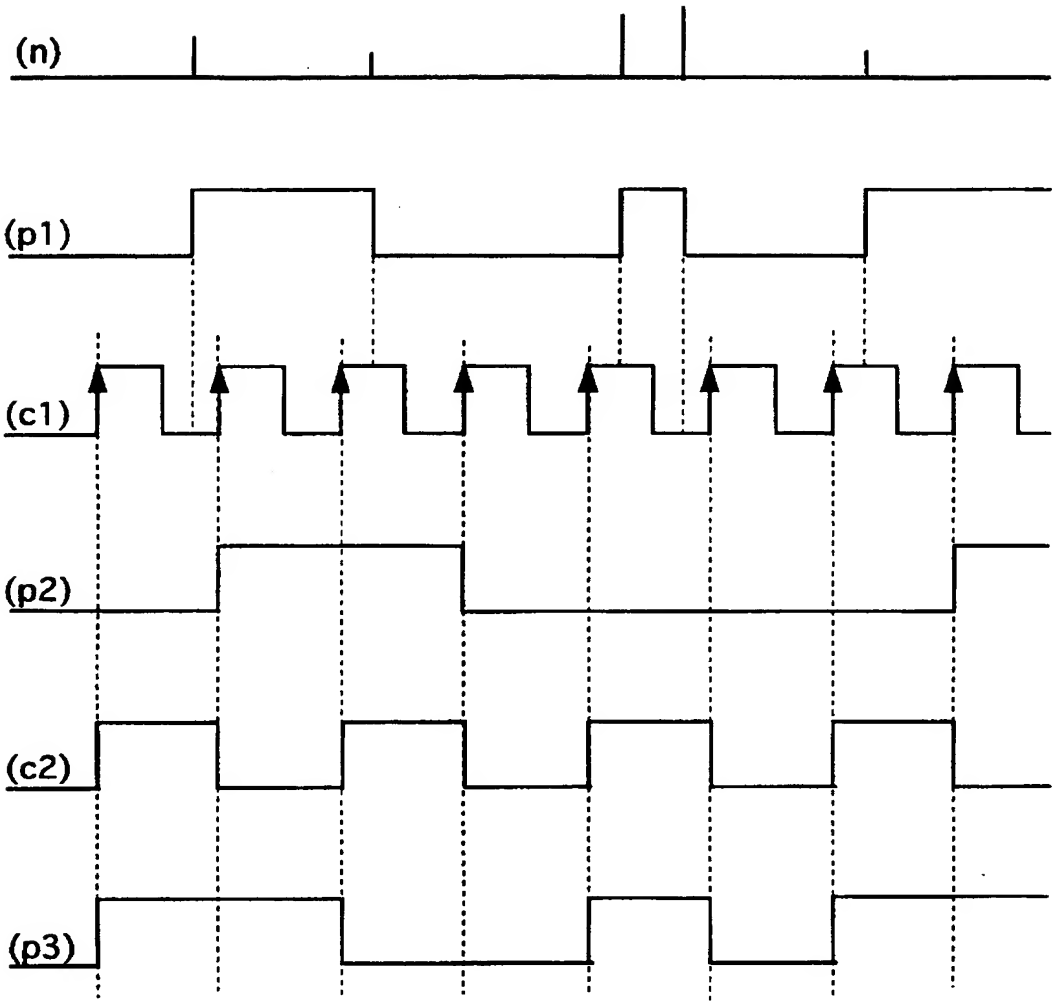
6　スイッチング回路

【書類名】　図面

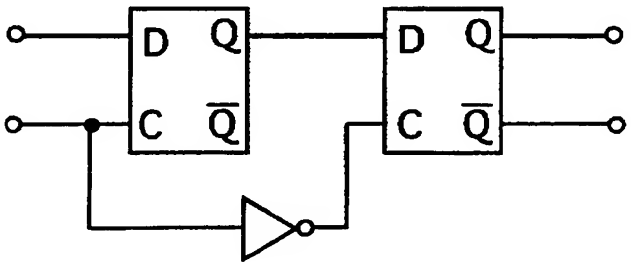
【図１】



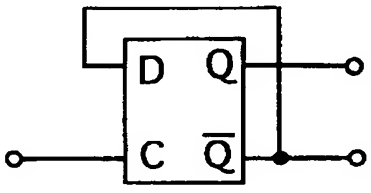
【図２】



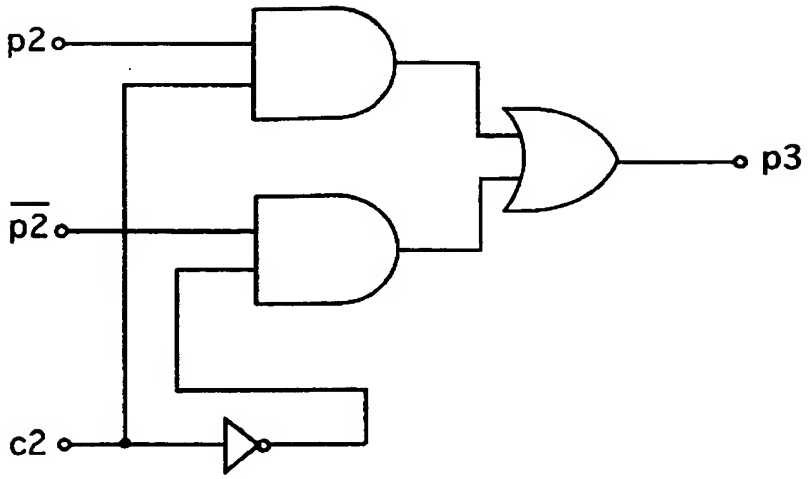
【図３】



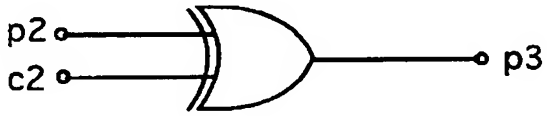
【図４】



【図５】



【図６】



【書類名】　　要約書

【要約】

【課題】偶然性に支配されることなく物理乱数のインバランスを解消して確実に１／０の出現バランスを等確率にできる乱数発生装置を提供する。

【解決手段】雑音源１が発生する周期性のないランダム雑音ｎを波形整形回路２に入力してランダムパルス波ｐ１を生成し、次に、ランダムパルス波ｐ１と発振器３のクロックｃ１をサンプル＆ホールド回路４に入力して一定周期の２値パルス列ｐ２を生成し、その２値パルス列ｐ２とクロックｃ１を分周器５で１／２に分周した１／２分周クロックｃ２をスイッチング回路６に入力して２値パルス列ｐ２の極性を１周期おきに反転させ、１／０符号の出現バランスを平滑化した平滑２値パルス列ｐ３を出力する。

【選択図】　　図１

特願２００１－１６３４２８

出　願　人　履　歴　情　報

識別番号　　［５９５０９５３５３］

１．変更年月日　　１９９７年１２月　８日
［変更理由］　　住所変更
住　所　　神奈川県横浜市都筑区池辺町字山王前４５０９番地
氏　名　　株式会社三技協

特願２００１－１６３４２８

出　願　人　履　歴　情　報

識別番号　［５００４５９２９２］

１．変更年月日　２０００年　８月２８日
［変更理由］　新規登録
住　所　神奈川県相模原市北里２－１７－２７
氏　名　株式会社サンテクト